## <u>Claims</u>

	1	<ol> <li>A method for retrieving digital objects from a group of digital objects</li> </ol>
	2	maintained by a database, the group of digital objects being represented by the equation
	3	$G = \{m_i, i = 1, 2,, N\}$ , wherein G represents the group of digital objects, N represents
٠	4	the number of digital objects maintained by the database, i represents an index having
	5	allowable values between 1 and N inclusive, and m, represents an ith digital object
	6	within the group of digital objects, the method comprising:
Brute S Gade	7	generating a random number R and keys k, i having allowable values between 1
dinit dask	8	and N inclusive, for a symmetric key cryptosystem;
in Sum	9	determining a prime number p;
William William	10	encrypting digital object m, with key k, using the symmetric key cryptosystem to
the state	11	obtain ciphertext c;
Amir M Godf	12	assigning a value of $k_i^R$ mod p to a key ciphertext $s_{i_i}$
######################################	13	responsive to the database receiving a request signal from a user, sending c, and
Harte Grave	14	s, to the user;
	15	receiving from the user a number n of input signals $W_{\mu}$ such that n is less than N,
	16	and j is an index having allowable values between 1 and n inclusive;
	17	computing changed ciphertext $U_{ij}$ such that $U_{ij}$ is equal to $W_{ij}^{1/2  \text{mod}  (p-1)}$ mod $p$ ; and
	18	sending U, to the user.
	_	
,	1	2. The method of claim 1, where the modulo operations may be carried out
	2	in any group in which a discrete logarithm is infeasible to compute.

Park Suit
1 1
dink dust
145 50 115
100
the state
=4
115
735 22 (32
3.5
11.
arma Sensiti
in in

1	3. A method for a user to privately retrieve digital objects from a group of
2	digital objects $G = \{ m_v i = 1, 2,, N \}$ maintained by a database, the method comprising
- 3	the steps of:
4	sending a request signal to the database;
5	receiving reply signals $c_v s_v l = 1, 2,, N$ from the database;
6	generating random numbers $w_i$ , computing and sending $W_i = s_{ij}^{w_i} \mod p$ , $j = 1, 2$ ,
7	, n to the database;
<b>, q</b>	receiving signals $U_{j'}$ $j = 1, 2,, n$ from the database;
9	computing $k_{ij} = U_j^{1/w_j \mod (p-1)} \mod p$ , $j = 1, 2,, n$ ; and
10	decrypting $c_{ij}$ with $k_{ij}$ and a symmetric key cryptosystem to recover digital objects
11	$m_{y'} j = 1, 2,, n.$
1	4. The method of claim 3, wherein the modulo operations may be carried out
2	in any group in which a discrete logarithm is infeasible to compute.
1	5. A method for selectively retrieving digital objects from a database of
2	digital objects using a symmetric key cryptosystem, the method comprising:
( · 3	for each digital object in the database:
4	generating a unique key for the symmetric key cryptosystem;
5	associating the key with the digital object;
6	encrypting the digital object using the associated key and the
7	symmetric key cryptosystem to produce a ciphertext of the
8	digital object;
9	encrypting the associated key to obtain a ciphertext of the key;
10	transmitting the ciphertext of the digital object and the ciphertext of
11	the key associated with the digital object to a user;

	12	receiving at least one changed ciphertext of the keys associated with the digital
	13	objects in the database;
	14	decrypting each received changed ciphertext; and
	15	transmitting the decrypted received changed ciphertexts.
	16	
	1	6. A method for retrieving digital objects from a group of digital objects
	2	maintained by a database, the method comprising the steps of:
	3	selectively requesting a plurality of digital objects from the database;
7:3	4	receiving encrypted ciphertext digital objects from the database;
Spult of	5	receiving from the database encrypted ciphertext keys associated with the
H. Hama And Good	6	received ciphertext digital objects;
11.12	7	encrypting at least one of the encrypted ciphertext keys to obtain changed
Harty Mark	8	ciphertext keys;
Marya Ma Gardi	9	sending the changed ciphertext keys to the database;
# 12 A	10	receiving partially decrypted changed ciphertext keys from the database;
Hart day	11	decrypting the partially decrypted changed ciphertext keys; and
off wille	12	decrypting at least one of the received ciphertext digital objects using the
	13	decrypted keys.
	1	7. An apparatus comprising:
		I to a series of the series of
	2	a computerized database;
	3	coupled to the database, a computer user;
	4	coupled to the database, a transmitting module for transmitting data to the user;
	5	coupled to the database, a receiving module for receiving data from the user;
	6	coupled to the database, a random number generating module for generating
	7	random numbers:

(

	8	coupled to the database, a key generating module for generating cryptographic
	9	keys;
	10	coupled to the database, an encrypting module for encrypting data;
	11	coupled to the database, a decrypting module for decrypting data;
	12	coupled to the user, a requesting module for requesting data from the database;
	13	coupled to the user, a transmitting module, for transmitting data to the database;
	14	coupled to the user, a receiving module, for receiving data from the database;
the H. H. Sprint Graph Sport Graph	15	coupled to the user, a random number generating module for generating random
		numbers;
	17	coupled to the user, an encrypting module for encrypting data; and
	18	coupled to the user, a decrypting module for decrypting data.
	1	8. A computer program product stored on a computer readable medium for
then then	2	retrieving digital objects from a group of digital objects maintained by a database, the
22	3	computer program product controlling a processor coupled to the medium to perform
a dink	4 .	the operations of:
Mann allen	5	for each digital object in the database:
W (	6	generating a unique key for a symmetric key cryptosystem;
	7	associating the key with the digital object;
	8	encrypting the digital object using the associated key and the
	9	symmetric key cryptosystem to produce a ciphertext of the
	10	digital object;
	11	encrypting the associated key to obtain a ciphertext of the key;
	12	transmitting the ciphertext of the digital object and the ciphertext of
	13	the key associated with the digital object to a user;
	14	receiving at least one changed ciphertext of the keys associated with the digital
	15	objects in the database;

- decrypting each received changed ciphertext; and
- transmitting the decrypted received changed ciphertexts.